

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,	)	
Plaintiff,	)	8:13CR108
	)	
	)	
vs.	)	
	)	
	)	
KIRK COTTOM, et. al.	)	
Defendants.	)	
	)	

**GOVERNMENT’S BRIEF IN OPPOSITION TO DEFENDANTS’ MOTIONS TO  
SUPPRESS EVIDENCE RESULTING FROM SEARCH OF “ACTIVATING”  
COMPUTER AND APPLICATION OF WONG SUN DOCTRINE**

Prepared and Submitted by:

DEBORAH R. GILG  
United States Attorney  
for the District of Nebraska

MICHAEL P. NORRIS (#17765)  
Assistant U.S. Attorney  
1620 Dodge Street, Suite 1400  
Omaha, Nebraska 68102-1506  
Phone: (402) 661-3700

KEITH BECKER  
DOJ Trial Attorney  
1400 New York Ave NW 6th Floor  
Washington, DC 20530  
(202) 305-4104

SARAH CHANG  
DOJ Trial Attorney  
1400 New York Ave NW 6th Floor  
Washington, DC 20530  
(202) 353-4979

## **I. NATURE OF THE CASE**

A Grand Jury sitting in the District of Nebraska has returned a superseding indictment against Kirk Cottom and Kevin Pitman. (Dkt. No. 6). Count I charges Cottom and Pitman with the receipt and attempted receipt of child pornography, a violation of Title 18, United States Code, Sections 2252A(a)(2) & (b)(1). Count II charges each defendant with accessing child pornography with the intent to view, a violation of Title 18, United States Code, Section 2252A(a)(5)(B). The allegations pertain to each defendant's use of a child pornography website, "Website A," that operated on a network designed to allow its users to access websites anonymously. Cottom and Pitman have entered pleas of not guilty to the superseding indictment.

Cottom and Pitman have each filed a motion to suppress evidence resulting from the execution of search warrants in the District of Nebraska authorizing the use of a Network Investigative Technique ("NIT"), alleging that the government violated Fed. R. Crim. P. 41(f)(1)(C) and (D) and 18 U.S.C. § 3103a(b), by failing to provide timely notice or service of the warrants. The United States respectfully submits that delayed notice of the warrants was provided within the parameters set by the authorizing Court and that, in any event, suppression of evidence would not be an appropriate remedy because the defendants cannot demonstrate prejudice or reckless disregard of proper procedures.

## **II. FACTS**

### "Website A"

"Website A," whose name is known to the Grand Jury, was a child pornography website whose primary purpose was the advertisement and distribution of child pornography. It operated from August of 2012 until December of 2012. On November 15, 2012, the computer server hosting "Website A" was seized from a web-hosting facility in Bellevue, Nebraska. The website

remained operating in Omaha, Nebraska from November 18, 2012, until December 2, 2012, at which time "Website A" ceased to operate. Between November 18, 2012, and December 2, 2012, law enforcement agents observed electronic communications of users of "Website A." Before and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A," which are described below.

"Website A" was a website of a format known as an "image board" that allowed its users to upload and view images containing male and female children as young as infants being sexually exploited. An image board is a categorized repository for digital images. "Website A" did not require an individual user to register or create an account to view, upload, or comment on material located on the board itself. Any user who accessed "Website A" had full access to every page of the board. "Website A" was broken into categories that pertained to pre-teen boys, teen-aged boys, teen-aged girls, babies/toddlers, and fetishes. There were no sections reserved for postings of adult pornography. The discussion area contained image posts, requests for specific images or image types, and reports from users regarding problems with the board. When a user wished to access a particular category, the user simply clicked on a link on the site which directed the user to a web-page containing images uploaded into that particular category.

There were over 6,000 images available on "Website A." The vast majority of those images depicted minor children engaged in sexually explicit conduct with adults or other children, or minor children who were fully or partially nude and posed so as to expose their genitals.

"Website A" users utilized advanced technological means in order to undermine law enforcement's attempts to identify them. For example, "Website A" was technically designed to facilitate anonymous communication by its users. Only a user who had installed special software

on the user's computer could access "Website A." That software enabled the communications of "Website A" users to be routed through multiple computers in order prevent communications from being traced back to the users. In addition, logs of member activity on "Website A" contained only the IP addresses of the last computer through which the communications of a user were routed before the communications reached "Website A." It is not possible to trace such communications back through the network to the actual user who sent the communications. Thus, those IP address logs could not be used to locate and identify the users of "Website A."

#### The Search Warrant Authorizing use of the NIT

On November 17, 2012, the United States District Court for the District of Nebraska authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique ("NIT") on "Website A" in an attempt to identify the actual IP addresses and other identifying information of computers used to access "Website A."<sup>1</sup> The application in support of the search warrant, search warrant, return, and supporting affidavit are attached as Exhibit 1.<sup>2</sup> On November 18, 2013, an inventory was returned to the Court that specified that "[a] Network Investigative Technique (NIT), computer code, was installed on the website [Website A] . . . ." Ex. 1, p. 3.<sup>3</sup> Pursuant to that authorization, between November 18, 2012, and December 2, 2012, each time a user of "Website A" accessed any page in certain particularly described sections of "Website A," the NIT sent one or more communications to the user's computer which were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer accessing "Website A," its location, its user, and other information about the computer. That data included the computer's

---

<sup>1</sup> The warrant, warrant application and affidavit in support thereof refer to "Website A" as "Hidden Service B."

<sup>2</sup> All attachments will be filed separately under seal and provided to defense attorneys.

<sup>3</sup> Defendant Cottom incorrectly contends that no return of the warrant was provided. Cottom Mtn. to Supp. at 4.

actual IP address and the date and time that the NIT determined what that IP address was, a unique session identifier to distinguish the data from that of other computers, and the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86). The NIT did not deny the users access to “Website A” or the possession or use of the information delivered to the computer controlled by or known to the government, nor did the NIT permanently alter any software or programs on the user’s computer.

#### The Request for Delayed Notice

In a section of the affidavit titled “REQUEST FOR DELAYED NOTICE,” the affidavit in support of the search warrant application cited and described the delayed notice provisions of Rule 41 and 18 U.S.C. § 3013a, articulated in detail why delayed notice was necessary, and requested authorization to delay notice to the person whose computer the NIT was used upon. Ex. 1, S. Warr. Aff., ¶¶ 22-25. For instance, the affidavit requested that the Court “authorize the proposed use of the NIT without the prior announcement of its use” because “[a]nnouncing the use of the NIT could cause the members of [Website A] to undertake other measures to conceal their identity, or abandon the use of [Website A] completely, thereby defeating the purpose of the search.” *Id.* ¶ 22. The affidavit articulated that notice of the use of the NIT “would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing [Website A]” and therefore would “seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(1) and 18 U.S.C. § 2705).” *Id.* ¶ 23. The affidavit further articulated that “the investigation has not yet identified an appropriate person to

whom such notice can be given.” Id. ¶ 24. Accordingly, the affidavit requested “authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing [Website A] has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.” Id. ¶ 24 (emphasis added). Further, in a section of the affidavit titled “SEARCH AUTHORIZATION REQUESTS,” the affidavit reiterated its request that:

pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an “activating” computer that accessed [Website A] has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

Id. ¶ 30. The application for the search warrant also reiterated the request for delayed notice, checking the appropriate box on the warrant application indicating that “[d]elayed notice of 30 days . . . is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.” Ex. 1, App. for S. Warr., p. 1. The issuing magistrate judge granted that request, checking the box on the warrant itself to commemorate his finding that “immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial),” and authorizing “the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized for 30 days.” Ex. 1, S. Warr., p. 2.

#### Identification and Arrest of Defendant Cottom

According to data obtained from logs on “Website A,” monitoring by law enforcement, and the deployment of the NIT, on November 19, 2012, a computer with the IP address 69.207.147.71 accessed child pornography, including images involving prepubescent minors engaged in sexually explicit conduct, on “Website A.” During that session, the user of that

computer browsed “Website A” anonymously without having been signed in as a registered user of the site.

On November 26, 2012, in response to an FBI administrative subpoena requesting subscriber information for IP address 69.207.147.71 on November 19, 2012, Time Warner Cable identified the subscriber of the Internet account associated with IP address 69.207.147.71 as Kirk Cottom and the subscriber address as 248 Wahl Rd., Rochester, NY. Ex. 2. Time Warner stated in that response that “[w]e do not make any representations as to the identity of the individual who actually used the above IP address on the date and times in question.” Id. at p. 1.

On March 20, 2013, “John Doe #1 a/k/a the user of IP address 69.207.147.71 on November 19, 2012,” was indicted in the District of Nebraska on charges of receipt/attempted receipt and access with intent to view child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) & (b)(1) and 2252A(a)(5)(B). Dkt. No. 1.

On April 9, 2013, a U.S. magistrate judge authorized the search of the premises at 248 Wahl Rd., Rochester, NY, for evidence related to the investigation of the user of IP address 69.207.147.71 on November 19, 2012. A copy of that warrant, warrant application and supporting affidavit are attached as Exhibit 3. The affidavit in support of that warrant disclosed in detail the court-authorized use of the NIT to identify a computer with IP address 69.207.147.71 as having accessed child pornography on “Website A” on November 19, 2013. Ex. 3, S. Warr. Aff. ¶¶ 16-21.

Also on April 9, 2013, law enforcement agents executed that warrant and searched the premises at 248 Wahl Rd., Rochester, NY. Kirk Cottom was present in the home. He was interviewed and admitted using the network on which “Website A” operated and being the only person who lived at the residence. Located in the residence were two computers – a desktop and

a laptop – that Cottom admitted he used. A preliminary forensic examination of the desktop computer conducted during the search revealed approximately 1,400 images of child pornography and child erotica depicting minors ranging from prepubescent children to young teenagers within a directory of the computer hard drive containing the name “adama.” Cottom admitted to using the username “adama” as an alias. After the interview and preliminary search of the computer, Cottom was arrested on the post-Indictment warrant that had been issued charging “John Doe #1 a/k/a the user of IP address 69.207.147.71 on November 19, 2012.”

Following Cottom’s April 9, 2013, arrest, an identity and detention hearing was held on April 11, 2013, in the Western District of New York. A transcript of the April 11, 2013, hearing is attached as Exhibit 4. During that hearing, the search warrant for the defendant’s residence was marked as an exhibit. Ex. 4, p. 13. After the residential search warrant disclosing the court-authorized use of the NIT had been moved into evidence, an FBI special agent referenced the search warrant’s disclosure of the NIT during cross-examination by the defendant’s attorney:

But I guess I can talk about what was in the search warrant affidavit. Yes, my understanding is that the reason they know that is they used a procedure -- well, they took over the website that housed the child pornography, and they got the approval to leave those up and running, court authority. And then they were able to use a procedure that I'm not personally familiar with, all the technical aspects of it, but they were able to, through that procedure that's called an NIT procedure, or was able to somehow determine that that user of that IP address was the end access point, that they were actually -- whoever was using that IP address was the individual that was accessing that website at that date and time.

Ex. 4, p. 30. On April 15, 2013, a U.S. magistrate judge found probable cause to believe that Kirk Cottom was John Doe #1 as charged in the Indictment and arrest warrant. Cottom was

subsequently released on conditions and transferred to the District of Nebraska pursuant to Rule 5.

On May 17, 2013, discovery was provided to the defendant through counsel, including the search warrant and affidavit for the defendant's residence, which disclosed the use of the NIT to determine the IP address ultimately tied to the defendant.

#### Arrest of Defendant Pitman

According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on November 20, 26, 27, 28, 30, and December 2, 2012, a user with the IP address 99.73.230.93 accessed child pornography on "Website A," including images of prepubescent minors engaged in sexually explicit conduct. During that session, the user of that computer browsed "Website A" anonymously without having been signed in as a registered member of the site.

On November 27, 2012, in response to an FBI administrative subpoena requesting subscriber information regarding IP address 99.73.230.93 on November 20, 2012, AT&T Internet Services identified the subscriber of the Internet account associated with IP address 99.73.230.93 as Kevin Pitman and the subscriber address as 10505 South Interstate Highway 35, Apartment #1325, Austin, Texas. Ex. 5, p. 3.

On March 20, 2013, "John Doe #3 a/k/a the user of IP address 99.73.230.93 between November 20, 2012 and December 2, 2012," was indicted in the District of Nebraska on charges of receipt/attempted receipt and access with intent to view child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) & (b)(1) and 2252A(a)(5)(B). Dkt. No. 1.

On April 8, 2013, a U.S. magistrate judge authorized the search of the premises at 10505 South Interstate Highway 35, Apartment #1325, Austin, Texas, for evidence related to the investigation of the user of IP address 99.73.230.93 on November 20, 2012.

On April 9, 2013, law enforcement agents executed that warrant and searched the premises at 10505 South Interstate Highway 35, Apartment #1325, Austin, Texas. The sole occupant present was Kevin Pitman, who identified himself and advised agents that he was the only occupant of the residence. Located in the residence was a desktop computer, which Pitman acknowledged belonged to him. Preliminary examination of the computer led to the discovery of more than 400 images of known or suspected child pornography, including images that were available on "Website A." Also present on the computer was software required to access "Website A" as well as bookmarks to numerous websites on the same network that "Website A" operated on known to law enforcement to contain child pornography.

Following that search and also on April 9, 2013, a criminal complaint was filed in the District of Nebraska charging Kevin Pitman with receipt/attempted receipt and access with intent to view child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) & (b)(1) and 2252A(a)(5)(B). On April 9, 2013, the day of Pitman's initial appearance in the Western District of Texas, a copy of his arrest warrant, criminal complaint and the affidavit in support of that complaint, were filed in the Western District of Texas. No. 13-mj-192-ML, W.D. Tex., Dkt. No. 1. Those documents are attached as Exhibit 6. Within the affidavit in support of that complaint is a detailed account of the use of the NIT to identify Pitman's IP address. Ex. 6, ¶¶ 12-18.

Following his April 9, 2013 arrest, an identity hearing was held on April 11, 2013 and a detention hearing was held on April 16, 2013 in the Western District of Texas. Pitman was released on conditions and transferred to the District of Nebraska pursuant to Rule 5. On May

29, 2013, initial discovery was provided to Pitman through counsel. By this date, Pitman had received a copy of the complaint and search warrant affidavits disclosing the use of the NIT.

### **III. ARGUMENT**

#### **A. The Government Provided Notice Pursuant to Rule 41 and 18 U.S.C. § 3103a**

Rule 41(f)(3) allows for the delay of any notice required by Rule 41 “if the delay is authorized by statute.” 18 U.S.C. § 3103a(b) allows for any such notice to be delayed if:

- (1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial);
- (2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and
- (3) the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay..<sup>4</sup>

Here, the issuing magistrate granted the government’s request that notice be delayed for 30 days “after a user of an ‘activating’ computer that accessed [Website A] [had] been identified to a sufficient degree as to provide notice.” Ex. 1, ¶¶ 24, 30. The date on which that identification occurred to a sufficient degree in regards to both defendants was April 9, 2013, following the searches and interviews that took place at their respective residences that identified them as the proper person to whom notice should be given. The use of the NIT was disclosed to each defendant through documents and testimony provided during the course of identity and detention

---

<sup>4</sup> Under 18 U.S.C. 2705 (2), any of the following constitute an adverse result:

- (A) endangering the life or physical safety of an individual;
- (B) flight from prosecution;
- (C) destruction of or tampering with evidence;
- (D) intimidation of potential witnesses; or

hearings after their arrests and again by providing supporting documents disclosing the use of the NIT through discovery. Accordingly, no violation of Rule 41 or 18 U.S.C. § 3103a occurred in either defendant's case.

Although the NIT identified IP addresses of computers that accessed "Website A" on the respective dates charged, no notice was required at that point because there was no one identified to whom notice could be given. The NIT did not identify a person, the user of a computer that was searched or the computer itself – it only identified the IP address and operating system type of a computer used to access "Website A." That information is helpful, but not sufficient, to identify the actual user of the computer or the computer that was searched.

The subscriber information contained in the respective subpoena returns was also helpful, but not sufficient, to identify the actual user of the computer or the computer that was searched. As Time Warner's subpoena response made clear, their response to the subpoena only provided information about the subscriber of the Internet account associated with the subject IP address and made no "representations as to the identity of the individual who actually used the above IP address on the date and times in question." Ex. 2, p. 1. Further investigation, to include a search of the defendant's homes and interviews of each defendant, was necessary before a determination could be made as to the actual identities of the users behind the computers that accessed "Website A" on the dates charged.<sup>5</sup> Only after interviewing each defendant and preliminarily searching their homes and computers did law enforcement agents sufficiently identify them in order to arrest them as the individuals who actually accessed "Website A." Accordingly, the

---

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

<sup>5</sup> In the case of a residential search of a suspect address based on IP information, law enforcement must consider numerous contingencies in identifying the actual perpetrator of an offense under investigation, including but not limited to the possibility of multiple residents or computer users at the address or open/unsecured wireless connections. In fact, during his April 9, 2013, interview with law enforcement, Cottom told law enforcement that he

earliest point at which the individuals to whom notice could be given were identified was April 9, 2013. Giving notice within 30 days of that date was therefore consistent with the request made in the affidavit and the warrant itself.

**B. Exclusion of evidence is not the proper remedy because the defendant cannot establish prejudice or the reckless disregard of proper procedures**

Even assuming that the government did not provide timely notice to defendants of the execution of the NIT warrant, suppression is not the appropriate remedy here because the defendants can show neither prejudice nor reckless disregard of proper procedures. In fact, neither defendant articulates any actual prejudice from any delay in obtaining notice of the use of the NIT. Moreover, law enforcement agents acted in accordance with their articulated requests to the Court regarding when notice was to be given.

Because the exclusionary rule is a “blunt instrument,” courts are “wary in extending [it] . . . to violations which are not of constitutional magnitude.” United States v. Hornbeck, 118 F.3d 615, 618 (8th Cir. 1997) (quoting United States v. Burke, 517 F.2d 377, 386 (2d Cir. 1975)). Thus, noncompliance with Fed. R. Crim. P. 41 “does not automatically require the exclusion of evidence in a federal prosecution.” United States v. Spencer, 439 F.3d 905, 913 (8th Cir. 2006) (citing United States v. Schoenheit, 856 F.2d 74, 76 (8th Cir. 1988)). Rather, when the government fails to comply with the requirements of Fed. R. Crim. P. 41, exclusion is warranted only if: (1) the defendant can demonstrate that he was prejudiced by the noncompliance, or (2) reckless disregard of proper procedures is evident. Spencer, 439 F.3d at 913; United States v. Nichols, 344 F.3d 793, 799 (8th Cir. 2003). The defendants can show neither.

---

“typically kept his wireless internet access secure, but at times he . . . maybe made mistakes and had it open where others could possibly use it.” Ex. 4, p. 20.

Prejudice, for the purposes of this inquiry, means “that the search might not have occurred or would not have been so abrasive if the Rule had been followed.” United States v. Burgard, 551 F.2d 190, 193 (8th Cir. 1977) (quoting United States v. Burke, 517 F.3d 377, 386-87 (2nd Cir. 1975)); see also, Schoenheit, 856 F.2d at 77; United States v. Brown, 584 F.2d 252, 258 (8th Cir. 1978). The defendants do not, and cannot, make such a showing. The warrant on its face authorized a delay in notice until after the search took place. Accordingly, the search would have occurred regardless of any delay in providing notice. Moreover, the search would have resulted in the collection of the exact same data – i.e., been just as “abrasive” – even if notice had been provided within 30 days from when the defendants claim notice should have been given. Thus, neither defendant suffered any actual prejudice from any delayed notice. The denial of motions to suppress has routinely been upheld where the defendant fails, as here, to establish prejudice from a failure in the execution of a search warrant. See Nichols, 344 F.3d 793, 799 (8th Cir. 2003) (affirming denial of suppression motion where defendant failed to establish prejudice from claimed inadequacies in search warrant inventory list); United States v. Reisselman, 646 F.3d 1072, 1078 (8th Cir. 2011) (affirming denial of suppression motion where defendant failed to establish prejudice from officer’s failure to provide warrant attachment to defendant at time of search).

Whether agents acted in reckless disregard of proper procedures is essentially a bad faith inquiry. See United States v. Bieri, 21 F.3d 811, 816 (8th Cir. 1994) (“[B]ecause no evidence exists that the officers acted in bad faith, it follows that there was no reckless disregard of proper procedure by the state officers.”); United States v. Hyten, 5 F.3d 1154, 1157 (8th Cir. 1993) (“our prior determination that [agents] acted in good faith precludes any finding of reckless disregard of proper procedure on their part.”); United States v. Berry, 113 F.3d 121, 123 (8th Cir. 1997)

(holding officers lack of bad faith in executing warrant at night without proper provision in warrant meant officers did not act in reckless disregard of proper procedure). There is no indication of any bad faith on behalf of the agents here. To the contrary, the search warrant affidavit specifically and explicitly disclosed the need for and request to delay notice until after a person to whom notice could be given was identified. That explicit request demonstrates good faith on behalf of the agents. See United States v. Mutschelknaus, 592 F.3d 826, 830 (8th Cir. 2010) (“the officers’ explicit request for an extension [of time to examine a computer pursuant to search warrant] shows a manifest *regard* for the issuing judge’s role in authorizing searches, rather than a bad faith [attempt] to circumvent federal requirements.” (emphasis in original) (internal citations omitted)). Moreover, notice was in fact provided to each defendant upon their identification as the proper person to whom notice was to be given.

Both defendants cite to United States v. Freitas, 800 F.2d 1451 (9th Cir. 1986), in an effort to analogize law enforcement’s conduct in this case to the actual, physical surreptitious entry by law enforcement into a criminal suspect’s home to seize “intangibles” such as the defendants’ actual IP addresses. Their reliance on Freitas is unavailing. While Freitas cautions that surreptitious entries into a person’s home by law enforcement should be “closely circumscribed,” in that case the Ninth Circuit overturned the trial court’s suppression of evidence obtained after law enforcement executed a warrant that allowed a surreptitious entry into a suspect’s home where the warrant lacked a notice requirement or a description of the property to be seized. Freitas, 800 F.2d at 1456-57. Moreover, the Ninth Circuit in Freitas found that the trial court should have applied the good faith exception, see generally United States v. Leon, 468 U.S. 897 (1984), to the officers’ conduct. Id. at 1457.<sup>6</sup>

---

<sup>6</sup> In the first place, the Fourth Amendment does not prohibit per se a covert physical entry even into a suspect’s home

In any event, this case did not involve any actual, physical surreptitious entry into either defendant's home pursuant to the NIT authorization. Rather, the NIT merely collected information – the computer's actual IP address and the type of operating system running on the computer – in which the defendants had no reasonable expectation of privacy. See United States v. Suing, 712 F.3d 1209, 1213 (8th Cir. 2013) (defendant "had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers.") (citing United States v. Stults, 575 F.3d 834, 842 (8th Cir. 2009) and United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008)).

Moreover, no seizure of any property took place pursuant to the NIT authorization. A seizure of property under the Fourth Amendment occurs when there is "some meaningful interference with an individual's possessory interests in that property." Dixon v. Lowery, 302 F.3d 857, 862 (8th Cir. 2002) (quotation marks and citation omitted). Not "every governmental interference with a person's property constitutes a seizure of that property under the Constitution." United States v. Va Lerie, 424 F.3d 694, 702 (8th Cir.2005) (en banc). The Fourth Amendment only prohibits the government's "conversion of an individual's private property" rather than "mere technical trespass to an individual's private property" or "inconsequential interference with an individual's possessory interests." Id. In merely collecting a user's IP address and computer operating system type, the NIT did not deny the defendants access to their computers, access to "Website A," or the possession or use of the IP address and operating system information collected by the NIT. Nor did the NIT permanently alter any software or programs on the user's computer. It merely recorded information about the user and

---

without advance notice to install surveillance equipment. See Dalia v. United States, 441 U.S. 238, 247-48 (1979). Nor does the Fourth Amendment or Rule 41 prohibit a search aimed at obtaining intangible information such as IP addresses. See United States v. New York Tel. Co., 434 U.S. 159, 169 (1977).

the computer. Such a recording of information does not constitute a seizure. See Arizona v. Hicks, 480 U.S. 321, 324 (1987) (recording of stereo equipment serial number while present in home is not a “seizure” because it did not meaningfully interfere with defendant’s possessory interest in the serial number or equipment).

#### **IV. CONCLUSION**

The defendants were provided timely notice of the use of the NIT to collect information from their computers and, in any event, cannot establish any prejudice or reckless disregard of the notice procedures of Rule 41 and 18 U.S.C. § 3103a. Accordingly, the Court should deny their motions to suppress.

WHEREFORE, the United States respectfully prays this Honorable Court to deny the defendants’ motions to suppress in this case.

Respectfully submitted,

---

MICHAEL P. NORRIS  
ASSISTANT U.S. ATTORNEY

---

SARAH CHANG  
TRIAL ATTORNEY

---

KEITH BECKER  
TRIAL ATTORNEY

CERTIFICATE OF SERVICE

I hereby certify that I have caused a copy of this motion to be sent to counsel for defendant, Julie A. Frank and Joseph F. Gross, Jr., via e-mail on November 1, 2013, to [jfrank1@cox.net](mailto:jfrank1@cox.net) and [jfgross@tjplaw.com](mailto:jfgross@tjplaw.com).

---

MICHAEL P. NORRIS  
ASSISTANT U.S. ATTORNEY